МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учебно-методическое объединение по естественнонаучному образованию

УТВЕРЖДАЮ
Первый заместитель Министра
образования Республики Беларусь
_____И.А.Старовойтова
«_____»_____ 2018 г.
Регистрационный № ТД-_____/тип.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Типовая учебная программа по учебной дисциплине

для специальности

1-31 03 07 Прикладная информатика (программное обеспечение компьютерных систем)

СОГЛАСОВАНО
Председатель Учебно-
методического объединения по
естественнонаучному образованию
_____ О.А. Ивашкевич
«____» _____ 2018 г.

СОГЛАСОВАНО
Начальник Главного управления
профессионального образования
Министерства образования
Республики Беларусь
_____ А.С. Касперович
«____» _____ 2018 г.

СОГЛАСОВАНО
Проректор по научно-методической
работе Государственного
учреждения образования
«Республиканский институт высшей
школы»
_____ И.В. Титович
«____» _____ 2018 г.

Эксперт-нормоконтролер
_____ _____
«____» _____ 2018 г.

Минск 2018

СОСТАВИТЕЛИ:

К.А.ЗУБОВИЧ, доцент кафедры технологий программирования Белорусского государственного университета, кандидат физико-математических наук, доцент

РЕЦЕНЗЕНТЫ:

Кафедра интеллектуальных информационных технологий Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»;

Ю.И.Иванченко, заведующий НИЛ прикладной информатики НИИ прикладных проблем математики и информатики, кандидат технических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:

Кафедрой технологий программирования Белорусского государственного университета
(протокол № 12 от 17 мая 2018 г.).

Научно-методическим Советом Белорусского государственного университета (протокол № 6 от 16 июня 2018 г.).

Научно-методическим Советом по прикладной математике и информатике учебно-методического объединения по естественнонаучному образованию (протокол № 16 от 29 мая 2018 г.).

Ответственный за редакцию: К.А.Зубович

Ответственный за выпуск: К.А.Зубович

Пояснительная записка

Типовая учебная программа по учебной дисциплине «Безопасность информационных систем» разработана в соответствии с типовым учебным планом и образовательным стандартом высшего образования первой ступени по специальности 1-31 03 07 «Прикладная информатика (по направлениям)» (ОСВО 1-31 03 07 – 2013).

В настоящее время одним из важнейших требований, предъявляемым к разрабатываемым, внедряемым и используемым системам создания, хранения и передачи данных (далее - «Информационные системы» («Information systems»), является их защищенность от «несанкционированного» использования (далее - «безопасность информационных систем» - «Information systems security»). Основной спецификой предметной области дисциплины «Безопасность информационных систем» является то, что она находится на стыке нескольких областей знаний, определяющих квалификацию современного специалиста в том, что называется «Прикладная информатика (программное обеспечение компьютерных систем)». В первую очередь, имеются ввиду такие области как: «Математика» (необходимость изучения, исследования и применения для защиты данных криптографических алгоритмов), «Информатика» (основы построения вычислительных систем и соответствующих программных средств, используемых в процессе создания, хранения и передачи данных), «Правоведение» (необходимость учета таких аспектов защиты информации как авторское право, административная и уголовная наказуемость противоправных действий с точки зрения несанкционированного использования систем хранения и передачи данных), «Психология» (как основа определения возможных поведенческих характеристик не только «злоумышленников», посягающих на тайны и средства пользователей информационных систем, не только разработчиков «зловредного» программного обеспечения, но и самих пользователей подобных систем). В связи с чем, дисциплина «Безопасность информационных систем» является важнейшей составной частью в подготовке специалистов в области прикладной математики и информатики

Дисциплина «Безопасность информационных систем» позволяет студентам получить следующие знания, навыки и умения. Во-первых, рассматриваются основы безопасности компьютерных систем и сетей: классифицируются угрозы, существующие в настоящее время для информационных систем, определяются механизмы нанесения ущерба, методы и средства противодействия угрозам и атакам, осуществляется ранжирование информации с точки зрения необходимости в её защите. Во-вторых, рассматриваются, изучаются модели безопасности и возможные архитектуры построения систем защиты данных. В-третьих, преподаются некоторые элементы криптографии (к сожалению, более тщательное изучение основ данной дисциплины требует отдельного рассмотрения в рамках других

курсов). В-четвертых, изучаются так называемые «Firewalls» (защитные экраны). В-пятых, анализируются существующие методы обнаружения вторжений и принципы построения «превентивных систем». В-шестых, рассматриваются аспекты защиты данных в коммерческих системах с акцентацией внимания на банковской деятельности и на электронной торговле. В-седьмых, классифицируются угрозы и методы противодействия им в рамках осуществления беспроводной передачи данных и передачи данных в локальных и глобальных сетях. В-восьмых, изучаются основы безопасности операционных систем (на примере Microsoft), систем управления базами данных, анализируются методы и средства «безопасного программирования» (разработки программного обеспечения для систем обеспечения защиты данных, с одной стороны, и разработки программного обеспечения, защищенного от взлома и (или) копирования, с другой). В-девятых, предлагаются к рассмотрению организационные, правовые, социальные аспекты построения систем защиты данных, включая этические нормы поведения в процессе эксплуатации информационных систем. В-десятых, описываются существующие в настоящее время подходы к стандартизации процессов обеспечения безопасности на различных предприятиях и в организациях.

Цель учебной дисциплины «Безопасность информационных систем»: формирование у студентов фундаментальных знаний и приобретение студентами практических навыков в области разработки программных продуктов, ориентированных на обеспечение безопасности систем обработки данных, защищенных от несанкционированного использования.

Образовательная цель: формирование необходимой для специалиста в области разработки программных средств совокупности знаний и практических навыков.

Развивающая цель: ориентирование студентов на необходимость развития способностей к самостоятельному решению проблем, возникающих в процессе повседневной деятельности в области разработки программных средств зашиты данных, формирование у студентов основ «хорошего рассказывания», на применение принципов «Разделяй и властвуй», на использование принципа «трех компасов» для определения истинности тех или иных заключений и решений при разработке систем обеспечения безопасности.

Основные задачи, решаемые при изучении дисциплины «Безопасность информационных систем»:

– Исследование предметной области под названием: «Обеспечение безопасности систем обработки данных»;

– Изучение методов и средств защиты данных, используемых в настоящее время в информационных системах;

– Изучение архитектуры компьютера, машинного языка, языков записи алгоритмов, позволяющих строить защиту данных на уровне, наиболее приближенном к аппаратному уровню;

– Изучение основ стандартизации в области безопасности информационных систем.

В результате изучения дисциплины студент должен:

знать:

– основные понятия в области информационных систем, правила их построения, основные компоненты подобных систем и принципы их функционирования;
– виды угроз для вычислительных систем, классификацию существующих программных средств, угрожающих целостности, конфиденциальности и доступности защищаемых данных;
– подходы к стандартизации средств защиты данных и к стандартизации систем информационной безопасности;
– административные, правовые, организационные и программно-аппаратные средства обеспечения безопасности информационных систем;
– принципы построения и функционирования программного обеспечения, защищенного от несанкционированного использования;

уметь:

– классифицировать угрозы безопасности информационной системы, отличать «вирус» от «троянского коня» и (или) «логической бомбы»;

– описывать «политику безопасности» с целью построения системы безопасности на конкретном предприятии;

– разрабатывать простейшие программные продукты, защищенные от несанкционированного использования;

– применять существующие в настоящее время программные средства защиты данных в вычислительных системах (TrueCrypt) и мобильные носители (flash-устройства) с соответствующим программным обеспечением;

владеть:

– основными средствами разработки программного обеспечения, ориентированного на защиту данных;

– навыками администрирования операционных систем с элементами обеспечения безопасности информации на примере Windows;

– методами и средствами построения программных средств, защищенных от несанкционированного использования.

Требования к академическим компетенциям специалиста

АК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

Требования к социально-личностным компетенциям специалиста

СЛК-3. Обладать способностью к межличностным коммуникациям.

СЛК-6. Уметь работать в команде.

Специалист должен быть способен:

Научно-исследовательская деятельность

ПК-8. Разрабатывать, эксплуатировать и сопровождать соответствующие программные компьютерные системы.

Проектно-конструкторская деятельность

ПК-11. Владеть алгоритмическим мышлением и современными языками программирования для программной реализации алгоритмов решения задач.

Организационно-управленческая деятельность

ПК-29. Контролировать и поддерживать трудовую и производственную дисциплину.

В соответствии со стандартом специальности 1-31 03 07-01 «Прикладная информатика (программное обеспечение компьютерных систем)», учебная программа предусматривает для изучения дисциплины 158 часов, из которых 68 аудиторных часа, в том числе лекционных – 34 часа, лабораторных – 34 часа.

Примерный тематический план

Название раздела	Количество аудиторных часов		
	Всего	В том числе	
		Лекции	Лабораторные занятия
Раздел I. Основные понятия в области теории информации и защиты данных в информационных системах	8	4	4
Раздел II. Классификация угроз, методы обнаружения вторжений, методы и средства защиты данных. Примеры	8	4	4
Раздел III. Организационные и правовые аспекты защиты данных. Политика безопасности. Стандарты в области обеспечения безопасности информационных систем	8	4	4
Раздел IV. Программные и аппаратные средства защиты данных в информационных системах	12	6	6
Раздел V. Построение защищенных вычислительных средств с использованием современных операционных систем, систем управления базами данных и языков программирования	12	8	4
Раздел VI. Обеспечение сетевой безопасности и защита данных с использованием мобильных устройств их хранения	8	2	6
Раздел VII. Разработка программного обеспечения систем защиты данных	12	6	6
Всего	68	34	34

Содержание учебного материала

Раздел I. Основные понятия в области теории информации и защиты данных в информационных системах

Определение информации, данных. Понятие системы, информационной системы. Определение архитектуры системы, основных компонент модельной информационной системы. Понятие и принципы защиты данных. Конфиденциальность, целостность и доступность информации как основные параметры защищенности данных. Постулаты защищенности информационных систем. Необходимые и достаточные условия для построения систем защиты данных. Классификация защищаемой информации.

Раздел II. Классификация угроз, методы обнаружения вторжений, методы и средства защиты данных. Примеры

Внутренние и внешние угрозы, классификация вредоносного программного обеспечения: вирусы, логические бомбы, «шпионские программы», «трояны» - определение и исследование. Резидентные программы и средства их обнаружения и локализации, описание основных антивирусных программных средств на примере Nod32. Пример разработки «вируса» и соответствующей антивирусной программы.

Раздел III. Организационные и правовые аспекты защиты данных. Политика безопасности. Стандарты в области обеспечения безопасности информационных систем

Основные понятия и определения. Политика безопасности. Защита данных в коммерческих и государственных организациях. Управление, социология, психология, право, организация в защите данных от несанкционированного использования. Авторские права. Административное и уголовное право в защите данных. Стандартизация и сертификация (СТБ ISO 27000. СТБ 34.101.XX).

Раздел IV. Программные и аппаратные средства защиты данных в информационных системах

Методы и средства защиты данных, основанные на использовании криптографии. Стеганография. Основные стандарты, применяемые в программных средствах шифрования данных (AES, belt, ГОСТ 28147). Применение программного средства TrueCrypt. Аппаратные средства защиты данных на примере использования переносимых устройств хранения данных (flash-накопителей). Программные и аппаратные средства защиты данных от копирования. Примеры.

Раздел V. Построение защищенных вычислительных средств с использованием современных операционных систем, систем управления базами данных и языков программирования

Основные понятия. Администрирование операционных систем в контексте обеспечения безопасности. Фундаментальные концепции безопасности операционных систем: защищенные области, матрицы доступа, механизмы безопасности. Основы безопасности в Microsoft Windows (accounts, group policies, NTFS permission, audit). Примеры администрирования. Различные аспекты безопасности баз данных, их администрирования: permission, roles, views and stored procedures. Разработка программного обеспечения, защищенного от вторжения вредоносных программ и отладчиков.

Раздел VI. Обеспечение сетевой безопасности и защита данных с использованием мобильных устройств их хранения

Понятие Firewall и их использование. Фильтрация пакетов. Применение «переносимых устройств» (на примере Flash-устройств Transcend) для защиты от посягательств на доступ к конфиденциальным данным. Возможности «шифрования данных на аппаратном уровне» - мифы и реальности. «Беспроводная и мобильная» безопасность в сетях: GSM-security, Bluetooth-security.

Раздел VII. Разработка программного обеспечения систем защиты данных

Определение жизненного цикла программного обеспечения, технологии программирования, ориентированных на создание программ обеспечения защиты данных. Определение требований как основа необходимых и достаточных условий для начала работ по созданию программного обеспечения. Structured Analysis как базис для определения требований. Понятия: принципы хорошего рассказывания, контекст, viewpoint, графическое отображение процессов. Реализация одного из постулатов в области защиты данных: чем на более близком к аппаратному уровню в контексте вычислительной техники осуществлена реализация системы защиты данных, тем она более эффективна – на примере разработки программы, удаляющей саму себя в рамках операционной системы Windows.

Информационно-методическая часть

Литература

Основная

1. Закон Республики Беларусь № 455-З от 10.11.2008 г. «Об информации, информатизации и защите информации (Национальный реестр правовых актов Республики Беларусь, 2008 г, № 279, 2/155. http://pravo.by/document/?guid=12551&p0=H11400102&p1=1.

https://normativka.by/lib/document/500066195/sid/5b93f5cc6a874b3ba977f2fbaf8b6e57.

2. Информационное право: учебник для студенческих учреждений высшего образования по юридическим специальностям/[авт.: Г.А. Василевич и др]; под общ. Ред. Г.А. Василевича, Д.А. Плетнева – Минск: Адукацыя і выхаванне, 2015. -391 с.
3. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. М.: ООО «Ленанд», 2015. - 248 с.
4. Национальный интернет-портал Республики Беларусь [Электронный ресурс]/Национальный центр правовой информации Республики Беларусь. -Минск, 2018.- Режим доступа: http://www.pravo.by. – Дата доступа 10.05.2018.
5. Национальный фонд технических нормативных правовых актов Республики Беларусь [Электронный ресурс]/Государственный комитет по стандартизации Республики Беларусь. - Минск, 2018. Режим доступа: http://www.tnpa.by.- Дата доступа 10.05.2018.
6. Интернет-портал международной организации по стандартизации [Электронный ресурс]/Международная организация по стандартизации. - Режим доступа: https://www.iso.org/ru/ Дата доступа 10.05.2018.
7. Вигерс Карл, Битти Джой. Разработка требований к программному обеспечению. 3-е изд. дополненное/ Пер. с англ. – М.: Издательство «Русская редакция»; СПб. :БХВ-Петербург, 2014. – 736 стр.: ил.
8. Ховард М., Лебланк Д. Защищенный код/ Пер. с англ., - 2-е изд, испр. М.: Издательско-торговый дом «Русская Редакция», 2004. – 704 стр.: ил.
9. Ховард М., Лебланк Д., Вьега Дж. 24 смертных греха компьютерной безопасности. Как написать безопасный код / Изд. Питер, 2010. – 400 с.
10. Стив Макконнелл. Совершенный код. Практическое руководство по разработке программного обеспечения. Мастер-класс/ Пер. с англ. – М.: Издательство «Ркссская Редакция»; СПб. : Питер, 2017.
11. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере. – М.: Форум, 2009.
12. Бурдаев О.В., М.А. Иванов, И.И. Тетерин. Ассемблер в задачах защиты информации. – М.: Кудиц-Образ, 2004.
13. Фленов М. Компьютер глазами хакера. – Санкт-Петербург, БХВ-Петербург, 2012
14. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. - М.: Диалог-МИФИ, 2003 – 256 с.
15. Требования и спецификации в разработке программ: сборник статей, перевод с английского. – М.: Мир, 1984
16. Казарин О.В. Безопасность программного обеспечения компьютерных систем. – Москва, МГУ, 2003, 212 с. – www.cryptografy.ru

Дополнительная

17. Марка Д.А., МакГоуэл К.М. Методология структурного анализа и проектирования SADT . – М.: Метатехнология, 1993.- 240с.
18. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: Монография. – Старый Оскол: ООО «ТНТ», 2005. – 448 с.
19. Krause M., Tipton H.F. Handbook of information Security Management. – CRC Press LLC. – www.cccure.com
20. The Red Book: A Roadmap for Systems Security Research. Seventh framework programme.- The SysSec Consortium. – www.syssec-project.eu
21. Boran S. IT Security CookBook. – www.boran.com/security
22. Указ Президента Республики Беларусь № 575 от 9 ноября 2010 г. «Об утверждении Концепции национальной безопасности Республики Беларусь. – www.pravo.by

Диагностика компетенций студента

На лекционных занятиях по дисциплине «Безопасность информационных систем» рекомендуется особое внимание обратить на точность формулировок и адекватность перевода англоязычных терминов на русский язык, так как неточные формулировки и перевод зачастую приводит к неверной трактовке тех или иных понятий в сфере безопасности информационных систем. В силу присутствия у студентов старших курсов различных подходов к пониманию материала, в начале семестра следует подробно остановиться на приведении к общему знаменателю их понятийного аппарата.

В силу различного уровня подготовки студентов старших курсов в области вычислительной техники и разработки программного обеспечения систем защиты данных, в самом начале обучения рекомендуется провести ряд самостоятельных работ и «ролевых игр» для определения этого уровня. И в зависимости от полученного результата варьировать лекционную тематику и степень сложности лабораторных работ. Так, например, в случае высокой квалификации обучаемых в низкоуровневом программировании (отменное знание основ операционных систем и программирования на языке ассемблер) следует больше внимания уделить разработке программного обеспечения систем защиты данных, перенеся данный раздел в начало семестра.

Текущий контроль усвоения знаний в течение семестра по дисциплине «Безопасность информационных систем» (теоретическая часть) рекомендуется осуществлять в виде проведения коллоквиума на четвертом месяце обучения. Для закрепления и проверки знаний и умений студентов (практическая часть) рекомендуется решение задач по каждому разделу дисциплины в виде выполнения ряда лабораторных работ, регулярного проведения самостоятельных работ, постоянного отслеживания процессов

выполнения студентами данных им работ непосредственно в компьютерном классе.

Успеваемость студентов в рамках дисциплины «Безопасность информационных систем» оценивается в конце семестра в форме экзамена.

Перечень рекомендуемых средств диагностики

В качестве основных средств диагностики компетенций студента предлагается использовать следующие:

1. Проведение в начале каждой лекции и лабораторной работы 5-минутных самостоятельных работ в письменном виде, необходимых для оценки уровня знаний, полученных за прошедшее с предыдущих занятий время.
2. Еженедельная отчетность о проделанной работе по выполнению лабораторных работ с размещением результатов в отдельной папке, датированной моментом сдачи отчета, причем в дальнейшем запрещается вносить изменения.
3. Выполнение упражнений, сформулированных в процессе чтения лекций и выполнения лабораторных работ, и пересылка результатов по электронной почте преподавателю.

Методические рекомендации по организации и выполнению самостоятельной работы

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются наличием и полной доступностью электронных (и бумажных) документов с указанием ссылок на первоисточники в рамках сети Интернет.

Использование при выполнении самостоятельной работы в процессе обучения принципа «трех компасов», когда для получения адекватного результата требуется изучение трех источников: 1. Средства массовой информации (книги, Интернет, лекции преподавателя, знания других студентов, знакомых, родственников и т.д. и т.п.) 2. «Здравый смысл» - собственные познания. 3. Результаты взаимодействия по решаемой проблеме с вычислительной техникой (результаты выполнения программ или результаты использования существующих программных средств).

Применение в процессе обучения подхода, основанного на том, что для организации самостоятельной работы и определения «уровня компетенции студентов» в процессе чтения лекций и при выполнении студентами лабораторных занятий, преподавателем выдвигаются «неверные» в контексте «трех компасов» утверждения (заведомо ложные»), которые должны быть опровергнуты обучаемыми.